Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims

1. (currently amended) A method of ~~determining~~ generating a result of a group operation, said method performed [[on]] by a computing apparatus an integral number of times on a selected element of a group, said group having a plurality of elements including a group identity element, said method comprising the steps of:

a) representing said integral number as a binary vector of bits having one value or another,

b) initialising said result to that of said group identity element;

c) selecting in sequence a predetermined number of successive bits of said vector and for each of said selected bits;

i) performing said group operation on said result to derive a first intermediate value,

ii) obtaining a second intermediate value by performing said group operation on said first intermediate value and said selected element when said computing apparatus is in one state and by performing said group operation on said intermediate value and an inverse of said selected element when said computing apparatus is in another state;

iii) replacing said result with said second intermediate value,

iv) selecting a state of said computing apparatus by examining an immediately preceding bit and maintaining the current state when said bits are of the same value and changing to

said other state when said bits are different;

d) repeating step c) for said predetermined number of said bits and performing said group operation on any remaining bits of said vector, whereby each of said predetermined bits of said of said vector is processed with ~~substantially equal~~ similar operations, thereby inhibiting disclosure of said sequence of predetermined bits to produce said result; and [[.]]

e) outputting said result for use in subsequent computations.

2. (currently amended) A method as defined in claim 1, said group being a ~~multiplicateive~~ multiplicative group F_p* said group element being an integer, and said group operation being exponentiation g^a and said inverse of said selected element having a value corresponding to a multiplicative inverse of said selected element.

3. (original) A method as defined in claim 1, said group being an additive group E (F_{2^m}) and said group operation being addition of points.

4. (previously presented) A method as defined in claim 1, said group being an additive group E (F_q), said group element being a point P with coordinates (x,y) on an elliptic curve, and said group operation being a scalar multiple kP of said point and an inverse element being a negative –P of said point.

5. (previously presented) A method as defined in claim 1, said integral number being a private key k used in a cryptosystem.

6. (currently amended) A method of performing a selected group ~~operating~~ operation on a scalar and a selected element of a group having a plurality of elements, to generate a result, [[in]] said method performed using a cryptographic processor[[, said method]] and comprising the steps of:

representing said scalar as a binary vector;

recoding said binary vector to produce a signed digit representation of plus one and minus one [[digist]] digits;

selecting each of said digits of said signed digit representation sequentially and for each of the selected digits performing said group ~~operating~~ operation on an intermediate element to derive a new intermediate element; and adding or subtracting a selected element of said group to said intermediate element in accordance with said signed digit representation [[being]] as each digit is selected; and

outputting said intermediate element as [[a]] said result of said group operation for use in subsequent computations.

7. (currently amended) A method according to claim 1 wherein said group operation is performed on said result and said inverse of said selected element if said last of said predetermined bits is one of said values.

8. (previously presented) A method according to claim 7 wherein said predetermined number of bits represents said entire vector.

9. (previously presented) A method according to claim 8 wherein said one of said values is representative of zero.